UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/468,621	12/21/1999	PIERRE STEVENS	21026.09	3845

7590 09/29/2003

Pierre Stevens
21047 Escondido Way
Boca Raton, FL 33433

EXAMINER
WU, ALLEN S

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/29/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/468,621	STEVENS, PIERRE	
	Examiner	Art Unit	
	Allen S. Wu	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-20 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-20 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 21 December 1999 is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Drawings

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: 836 (recharging interface, pg. 13 line 11), 812 (PIN, pg. 19 line 9), 121 (step, pg. 25 line 15). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "420" has been used to designate both counter (pg. 22 line 16) and step of processing PIN number (fig 5). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: 405 (fig 4), 450, 452, 442, 444 (fig 6), 1102, 1104, 1106, 1108, 1110, 1111, 1112, 1114, 1116, 1118, 1120 (fig 11), 1212, 1214, 1216, 1218, 1228 (fig 12) and 1302, 1310, 1312, 1314, 1316, 1318, 1320, 1322 (fig 13). A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in the description, are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Objections

4. Claim 9 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form.

In parent claim, claim 8, input means are stated as a key input, a voice audio input, a signature input, and a fingerprint input. Further limitations from claim 8 include a tone sequence corresponding to the stored representation of the user input. Claim 9 attempts to limit the tone sequence to comprise a representation of the captured at least one of a key input, a voice audio is input, a signature input, and a fingerprint input from a user of the secure access card to identify the user thereof. This limitation is already stated in claim 8 wherein the tone corresponds to the user input as a key input, a voice audio input, a signature input, and a fingerprint input. Claim 9 is a dependent claim of claim 8 and therefore does not place any further limitation on the tone sequence.

5. Claim 16 is objected to because of the following informalities: There is a grammatical error at the end of claim 16, page 33 line 18. The claim reads, to determine whether the user input identifies the user an authorized. The claim does not further describe what the user is authorized for (e.g. Authorized user of secure access function of a system, as in claim 8). Therefore, the claim is indefinite in its limitations. It is noted that the examiner assumes the claim to further read, authorized user of secure

access function of a system, as in claim 8, for the purposes of this office action. Appropriate correction is required.

6. Claim 19 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form.

Claim 18, parent of claim 19, claims a tone sequence corresponding to the user input. Claim 19 further limits the user input to at least one of a key input, a voice audio input, a signature input, and a fingerprint input. Therefore the tone sequence will correspond to the user input, which is limited in claim 19. Claim 20, child of claim 19, tries to further limit the tone sequence to comprise a representation of the captured at least one of a key input, a voice audio input, a signature input, and a fingerprint input. This limitation is already done through claims 18 and 19, which are parent claims to claim 20.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1-4, and 7 are rejected under 35 U.S.C. 102(b) as being anticipated by Mark, US Paten 5,583,933.

As per claim 1, Mark discloses a secure access card (auto-dialer, Abstract) at least one tone generator for generating at least one tone signal that is variable in at least one of tone frequency, time duration of tone, time duration of space between tones, and by amplitude of tone (col 5 ln 30-35); tone generator (DTMF encoder/generator, col 8 ln 23-34) comprising at least one acoustic transducer (speaker col 8, ln 34-55) that is mechanically tuned to oscillate about its mechanical resonant frequency to substantially maximize audio power output from at least one tone generator (DTMF generator produce tones of nominal frequency, col 24 ln 24-40, auto calibration of the auto dialer, col 24 lines 63-67 and col 21 ln1-9; It is well known in the art that a generator that produces tones of nominal frequency, intensity, and duration is known to be oscillating at its mechanical resonant frequency); input means for accepting input from a user (device keys, col 8 ln 10-17 and microphone, col 8 ln 23-33); and a controller (microprocessor, col 8 ln 10-17), electrically coupled to the at least one tone generator (speaker, col 8 ln 23-33) and the input means (device keys, col 8 ln 10-17 and microphone, col 8 ln 23-33), for controlling the at least one tone generator to generate a tone sequence corresponding to the input from the user (DTMF signal, col 5 ln 25-57, PIN corresponding to input, col 57 ln 13-22, and voice transmitted via encoded DTMF, col 50 ln 55-63).

As per claim 2, Mark discloses a secure access card (auto-dialer, Abstract) wherein the at least one tone generator generates a tone sequence comprising at least one of dual tone multi frequency (DTMF) signals, FSK

signals, MSK signals, and multitone signals (DTMF or other types including FSK, col 1 ln 23-36 and col 66 ln 39-45; FSK and MSK are multi tone signals that are used for data transmission, like DTMF signals and are well known in the art. Mark specifically teaches the use of DTMF signals but suggests similar signals also apply. FSK signals, MSK signals and other multi tone signals similar DTMF signals are to be inherent to the invention disclosed by Mark), signals to identify the user as authorized user(information transmitted to the network by a series of encoded DTMF tones and is compared to authenticate the user, col 50 ln 55-67 and col 51 ln 1-4). .

As per claim 3, Mark discloses at least one tone generator further comprises a controllable amplifier circuit (degree of amplification controlled by microprocessor, col 48 ln 33-50), the controller being electrically coupled to the controllable amplifier circuit and to the at least one acoustic transducer to selectively control the controllable amplifier circuit (Lo-band and Hi-band tone signals are amplified separately...through amplitude control signals, col 19 ln 44-56; degree of amplification controlled by microprocessor, col 13 ln 33-50) and the at least one acoustic transducer to generate the tone sequence corresponding to the input from the user (DTMF signal, col 50 ln 56-63; placement of call with correct PIN, col 57 ln 3-23) .

As per claim 4, Mark discloses tone generator generates a tone sequence (DTMF signal, col 50 ln 56-63; placement of call with correct PIN, col 57 ln 3-23) that is delivered via a communication network interface (telephone, col 5 ln 51-

59) comprising a telephone network interface for a publicly switched telephone network (PSTN) (telephone lines/system, col 5 ln 37-50; The auto-dialer is used for placing telephone calls through a publicly switched telephone network. Therefore a communication network interface comprising a telephone network interface for a publicly switched telephone network (PSTN) is to be inherent to the invention of Mark).

As per claim 7, Mark discloses memory for storing a representation of user input (RAM, col 8 ln 10-17; storage of a user's voice file, col 48 ln 33-50; PIN numbers and phrases, col 56 ln 39-52), and wherein the controller (microprocessor, col 8 ln 10-33) is electrically coupled to the memory and to the input means (microphone, col 8 ln 34-56) for monitoring the input means for user input and to store a representation of the user input in the memory (store voice identification or biometric information, col 50 ln 22-63) the controller controlling the at least one tone generator to generate a tone sequence corresponding to the stored representation of the user input (information transmitted to the network or facility by a series of encoded tones, col 50 ln 45-55), the tone sequence for delivery via a communication network interface to a secure access server to determine whether the user input identifies the user as an authorized user of secure access function of a system (access control device, col 50 ln 22-63 and col 51 ln 1-5).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mark, US Patent 5,583,933 in view of Paterno et al, US Patent 5,636,271.

As per claim 5 Mark discloses memory for storing identification information (RAM, col 8 ln 10-17; storage of a user's voice file, col 48 ln 33-50; PIN numbers and phrases, col 56 ln 39-52), and wherein the controller (microprocessor, col 8 ln 10-33) is electrically coupled to the to memory and to the input means (microphone, col 8 ln 34-56).

Mark does not teach the controller to monitor the input means for user input and to determine whether the user input matches the stored identification information to permit the card to generate the tone sequence for delivery via the communication network interface. However, Paterno et al. discloses an access card that monitors PIN input to determine whether the user input matches the stored identification information to permit the card to generate the tone sequence (DTMF tone representation of PIN, col 1 ln 63-67 and col 2 ln 1-13) for delivery via the communication network interface (telephone; col 1 ln 63-67 and col 2 ln 1-13). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to incorporate the teachings of Paterno et al within the

system of Mark because it would have added an extra security to the authentication process of the card and user before the card is used with the access control device of Mark's invention.

11. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mark, US Patent 5,583,933 in view of Paterno et al, US Patent 5,636,271, and further in view of Fung et al.

As per claim 6, Mark discloses input means comprising at least one of a key input, a voice audio input, and a fingerprint input (capturing and converting voice data/biometric data and transferring converted digital data to auto-dialer, col 48 ln 10-43).

Mark does not teach to determine whether the user input matches the stored identification information to permit the card to generate the tone sequence for delivery via the communication network interface. However, Paterno et al. discloses a access card that monitors PIN input to determine whether the user input matches the stored identification information to permit the card to generate the tone sequence (DTMF tone representation of PIN, col 1 ln 63-67 and col 2 ln 1-13) for delivery via the communication network interface (telephone; col 1 ln 63-67 and col 2 ln 1-13). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to incorporate the teachings of Paterno et al within the system of Mark because it would have added an extra

security to the authentication process of the card and user before the card is used with the access control device of Mark's invention.

Furthermore, the combination of Mark and Paterno does not teach user the input means comprising of a signature identification method. However Fung et al. discloses an ID system, which authorizes user with biometric input, including signature or other writing (col 5 section 0060). The secure access card uses the signature information of the user as authentication information to authorize the user to use the requested services. Fung et al teaches the use of biometric data, including written signature, to authenticate the user who is accessing downloaded content. The signature identification and other forms of identification have the same purpose of authenticating the user of the card. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Fung et al within the combination of Mark and Paterno because it would have added another set of data to authenticate the user.

12. Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mark, US Patent 5,583,933 in view of Fung et al.

As per claims 8 and 9, Mark discloses input means comprising at least one of a key input, a voice audio input, and a fingerprint input, to capture user input from a user of the secure access card and to store a representation of the user input in the memory (interfacing equipment ...accessing a record or group of records, which contain voice or other biometric details of the user col 55 ln 30-43;

supply set of PIN numbers through keypad of telephone, col 57 ln 3-12), the controller controlling the at least one tone generator to generate a tone sequence corresponding to the stored representation of the user input for delivery via a communication network interface to a secure access server to determine whether the user input identifies the user as an authorized user of secure access function of a system (information transmitted to the network of facility by a series of encoded DTMF tones, col 50 ln 55-67 and col 51 ln 1-4).

Mark does not teach user the input means comprising of a signature identification method. However Fung et al. discloses an ID system, which authorizes user with biometric input, including signature or other writing (col 5 section 0060). The secure access card uses the signature information of the user as authentication information to authorize the user to use the requested services. Fung et al teaches the use of biometric data, including written signature, to authenticate the user who is accessing downloaded content. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Fung et al within the system of Mark because it would have added another set of data to authenticate the user.

13. Claims 10-13, and 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mark, US Patent 5,583,933 in view of Fung et al, in further view of Maes et al.

As per claim 10, Mark discloses a communication network (telephone system, col 50 ln 22-27; network, col 50 ln 56-63); a secure application/function server, electrically coupled to the communication network, for providing secured access functions to an authorized user across the communication network (access control device granting access to individual seeking access to the system the requested access, col 50 ln 45-55); a secure access server (comparator on the access control device, col 50 ln 28-63), electrically coupled to the communication network, for determining whether a user across the communication network is an authorized user (compare biometric identification received to a live sample, col 50 ln 45-55; place call based on correct PIN, col 57 ln 3-23) a network interface for coupling communication signaling between the communication network and the secure access server (telephone and microphone/speaker of access control device, col 50 ln); a tone signal processor electrically coupled to the network interface for receiving and processing communication signaling from the communication network (DTMF encoder/decoder and microphone/speaker, col 50 ln 28-44), the communication signaling comprising at least one tone signal in a tone sequence (encoded DTMF tones, col 50 ln 56-63); a database memory for storing authorized user identification information (interfacing equipment ...accessing a record or group of records, which contain voice or other biometric details of the user (col 55 ln 30-43) including for each authorized user at least one of a personal identification number (PIN), a voice identification information, a fingerprint identification

information (biometric data, col 55 ln 30-43); a controller (microprocessor, col 50 ln 38-55), electrically coupled to the tone signal processor and the database memory, for receiving communication signaling from the communication network (microphone/decoder coupled to microprocessor to receive biometric identification via the input device, col 50 ln 28-37), the communication signaling comprising at least one tone signal in a tone sequence representative of user identification information (voice information sent through encoded DTMF tones, col 50 ln 56-63). It is noted that the purpose of a secure application/function server is to provide the authorized user the requested application/functions. The access control device, which is disclosed by Mark, grants access to the requested system, functions after authorization of user. Therefore the secure application/function server is to be inherent to the operation performed by the access device control of Mark's invention.

Furthermore, Mark discloses a secure access card (auto-dialer, Abstract) at least one tone generator for generating at least one tone signal that is variable in at least one of tone frequency, time duration of tone, time duration of space between tones, and by amplitude of tone (col 5 ln 30-35); tone generator (DTMF encoder/generator, col 8 ln 23-34) comprising at least one acoustic transducer (speaker col 8, ln 34-55) that is mechanically tuned to oscillate about its mechanical resonant frequency to substantially maximize audio power output from at least one tone generator (DTMF generator produce tones of nominal frequency, col 24 ln 24-40, auto calibration of the auto dialer, col 24 lines 63-67

and col 21 ln1-9; It is well known in the art that a generator that produces tones of nominal frequency, intensity, and duration is known to be oscillating at its mechanical resonant frequency); input means for accepting input from a user (device keys, col 8 ln 10-17 and microphone, col 8 ln 23-33); and a controller (microprocessor, col 8 ln 10-17), electrically coupled to the at least one tone generator (speaker, col 8 ln 23-33) and the input means (device keys, col 8 ln 10-17 and microphone, col 8 ln 23-33), for controlling the at least one tone generator to generate a tone sequence corresponding to the input from the user (DTMF signal, col 5 ln 25-57, PIN corresponding to input, col 57 ln 13-22, and voice transmitted via encoded DTMF, col 50 ln 55-63).

Mark does not teach user identification information for each user stored in the database to include a signature identification method. However Fung et al. discloses an ID system, which authorizes user with biometric input, including signature or other writing (col 5 section 0060). The secure access card uses the signature information of the user as authentication information to authorize the user to use the requested services. Fung et al teaches the use of biometric data, including written signature, to authenticate the user who is accessing downloaded content. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Fung et al within the system of Mark because it would have added another set of data to authenticate the user.

Furthermore, the combination of Mark and Fung et al does not teach comparing the user identification information to the stored authorized user identification information to determine whether the user identification information received from across the communication network corresponds to an authorized user for accessing secured access functions provided by the secure application/function server to an authorized user across the communication network. However, Maes discloses a central server that processes user input and authenticates user based on information pre-stored on the server (col 7 ln 20-35 and col 8 ln 12-27). Using the central server to compare and store the authorized user identification information would allow for more memory to store more information on different users, and would add an extra layer of security on top of the security of the access card. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Maes et al within the combination of Mark and Fung et al so that the central server, disclosed by Maes et al, can communicate with the auto dialer, disclosed by Mark, because it would have added additional user security to functions accessed by the card.

As per claim 11, Mark discloses a secure access card (auto-dialer, Abstract) wherein the at least one tone generator generates a tone sequence comprising at least one of dual tone multi frequency (DTMF) signals (DTMF or other types including FSK, col 1 ln 23-36 and col 66 ln 39-45) and signals to

identify the user as authorized user(information transmitted to the network by a series of encoded DTMF tones and is compared to authenticate the user, col 50 ln 55-67 and col 51 ln 1-4).

As per claim 12, Mark discloses at least one tone generator further comprises a controllable amplifier circuit (degree of amplification controlled by microprocessor, col 48 ln 33-50), the controller being electrically coupled to the controllable amplifier circuit and to the at least one acoustic transducer to selectively control the controllable amplifier circuit (Lo-band and Hi-band tone signals are amplified separately...through amplitude control signals, col 19 ln 44-56; degree of amplification controlled by microprocessor, col 13 ln 33-50) and the at least one acoustic transducer to generate the tone sequence corresponding to the input from the user (DTMF signal, col 50 ln 56-63; placement of call with correct PIN, col 57 ln 3-23) .

As per claim 13, Mark discloses tone generator generates a tone sequence (DTMF signal, col 50 ln 56-63; placement of call with correct PIN, col 57 ln 3-23) that is delivered via a communication network (telephone system, col 5 ln 37-50) comprising a telephone network interface for a publicly switched telephone network (PSTN) (telephone lines/system, col 5 ln 37-50; The auto-dialer is used for placing telephone calls through a publicly switched telephone network. Therefore, a communication network interface comprising a telephone

network interface for a publicly switched telephone network (PSTN) is to be inherent to the invention of Mark).

As per claim 16, Mark discloses memory for storing a representation of user input (RAM, col 8 ln 10-17; storage of a user's voice file, col 48 ln 33-50; PIN numbers and phrases, col 56 ln 39-52), and wherein the controller (microprocessor, col 8 ln 10-33) is electrically coupled to the memory and to the input means (microphone, col 8 ln 34-56) for monitoring the input means for user input and to store a representation of the user input in the memory (store voice identification or biometric information, col 50 ln 22-63) the controller controlling the at least one tone generator to generate a tone sequence corresponding to the stored representation of the user input (information transmitted to the network or facility by a series of encoded tones, col 50 ln 45-55), the tone sequence for delivery via a communication network interface to a secure access server to determine whether the user input identifies the user as an authorized user of secure access function of a system (access control device, col 50 ln 22-63 and col 51 ln 1-5).

As per claim 17, Mark discloses input means comprises at least one of a key input, a voice audio input, and a fingerprint input, to capture user input from a user of the secure access card and to store a representation of the user input in the memory (interfacing equipment ... accessing a record or group of records,

which contain voice or other biometric details of the user col 55 ln 30-43; supply set of PIN numbers through keypad of telephone, col 57 ln 3-12), the controller controlling the at least one tone generator to generate a tone sequence corresponding to the stored representation of the user input for delivery via a communication network to a secure access server to determine whether the user input identifies the user as an authorized user of secure access function of a system (information transmitted to the network of facility by a series of encoded DTMF tones, col 50 ln 55-67 and col 51 ln 1-4).

Mark does not teach user the input means comprising of a signature identification method. However Fung et al. discloses an ID system, which authorizes user with biometric input, including signature or other writing (col 5 section 0060). The secure access card uses the signature information of the user as authentication information to authorize the user to use the requested services. Fung et al teaches the use of biometric data, including written signature, to authenticate the user who is accessing downloaded content. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Fung et al within the system of Mark because it would have added another set of data to authenticate the user.

14. Claims 14 and 15 rejected under 35 U.S.C. 103(a) as being unpatentable over Mark, US Patent 5,583,933 in view of Fung et al, in further view of Maes et al., and in further view of Paterno et al, US Patent 5,636,271.

As per claim 14 Mark discloses memory for storing identification information (RAM, col 8 ln 10-17; storage of a user's voice file, col 48 ln 33-50; PIN numbers and phrases, col 56 ln 39-52), and wherein the controller (microprocessor, col 8 ln 10-33) is electrically coupled to the to memory and to the input means (microphone, col 8 ln 34-56).

The combination of Mark, Fung et al, and Maes et al does not teach the controller to monitor the input means for user input and to determine whether the user input matches the stored identification information to permit the card to generate the tone sequence for delivery via the communication network interface. However, Paterno et al. discloses an access card that monitors PIN input to determine whether the user input matches the stored identification information to permit the card to generate the tone sequence (DTMF tone representation of PIN, col 1 ln 63-67 and col 2 ln 1-13) for delivery via the communication network interface (telephone; col 1 ln 63-67 and col 2 ln 1-13). To have the controller determine if user input matches user information, already stored in the card, would require a reprogramming of the controller. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to incorporate the teachings of Paterno et al within the combination of Mark, Fung et al, and Maes et al because it would have added an extra security to the authentication process of the card and user before the card is used with the access control device of Mark's invention.

As per claim 15, Mark discloses input means comprising of at least one of a key input, a voice audio input, and a fingerprint input, to capture user input from a user of the secure access card (capturing and converting voice data/biometric data and transferring converted digital data to auto-dialer, col 48 ln 10-43; supply set of PIN numbers through keypad of telephone, col 57 ln 3-12; It is noted that Mark does not disclose the card physically capable of capturing and converting the data digitally. However, Mark discloses a method of capturing the data from a central office and transferring a digital representation of the data to the card. Both are ways different methods but result in the same outcome of voice and other biometric data being captured and stored in memory on the card).

Mark does not teach user the input means comprising of a signature identification method. However Fung et al. discloses an ID system, which authorizes user with biometric input, including signature or other writing (col 5 section 0060). The secure access card uses the signature information of the user as authentication information to authorize the user to use the requested services. Fung et al teaches the use of biometric data, including written signature, to authenticate the user who is accessing downloaded content. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Fung et al within the system of Mark because it would have added another set of data to authenticate the user and added extra security to the auto dialer Mark disclosed.

Furthermore, Mark does not teach the user input being compared to the stored identification information to permit the card to generate the tone sequence for delivery via the communication network interface. However, Paterno et al. discloses a access card that monitors PIN input to determine whether the user input matches the stored identification information to permit the card to generate the tone sequence (DTMF tone representation of PIN, col 1 ln 63-67 and col 2 ln 1-13) for delivery via the communication network interface (telephone; col 1 ln 63-67 and col 2 ln 1-13). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to incorporate the teachings of Paterno et al within the system of Mark because it would have added an extra security to the authentication process of the card and user before the card is used with the access control device of Mark's invention

15. Claim 18 rejected under 35 U.S.C. 103(a) as being unpatentable over Mark, US Patent 5,583,933, in view of Maes et al, US Patent 6,016,476.

As per claim 18, Mark discloses a communication system (telephone system, col 50 ln 23-27) comprising the steps of: capturing user input at a secure access card (storage of voice or other biometric information, col 50 ln 44-50; It is noted that storing the voice or biometric information on the access card requires a method of capturing such input. Therefore the capturing of user input is inherent to the teachings of Mark); storing a representation of the user input at the secure access card (storage of voice or other biometric information, col 50 ln

44-50); acoustically transmitting, from the card, a tone sequence destined for reception across a communication network (encoded DTMF tones, col 50 ln 55-63), the tone sequence corresponding to the stored representation of the user input (voice identification information may be transmitted to the network/access control device by a series of encoded DTMF tones, col 50 ln 55-63); receiving from across the communication network a representation of the to transmitted tone sequence (microphone and DTMF decoder for receiving and decoding encoded DTMF tones, col 50 ln 28-36); comparing (compare the voice data to voice sample, col 50 ln 45-55)

Mark does not teach comparing the received representation of the transmitted tone sequence to pre stored authorized user identification information; and determining whether a match between the representation of the transmitted tone sequence and a pre-stored authorized user identification information identifies the user is of the secure access card as an authorized user of the communication system. However, Maes et al discloses a central server that processes user input and authenticates user based on information pre-stored on the server and determines if the user is an authorized user of the communication system (col 7 ln 20-35 and col 8 ln 12-27). It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Maes et al within the system of Mark so that the central server, disclosed by Maes et al, can communicate with the auto dialer through

tone signals, discloses by Mark, because it would have added additional user security to functions accessed by the card.

16. Claims 19 and 20 rejected under 35 U.S.C. 103(a) as being unpatentable over Mark, US Patent 5,583,933, in view of Maes et al, US Patent 6,016,476, as applied to claim 18 above, and further in view of Fung et al.

As per claim 19, Mark discloses capturing at least one of a key input, a voice audio input, and a fingerprint input, to capture user input from a user of the secure access card (capturing and converting voice data/biometric data and transferring converted digital data to auto-dialer, col 48 ln 10-43; It is noted that Mark does not disclose the card physically capable of capturing and converting the data digitally. However, Mark discloses a method of capturing the data from a central office and transferring a digital representation of the data to the card. Both are different methods but result in the same outcome of voice and other biometric data being captured and stored in memory on the card. Therefore the method of capturing user input is inherent to the invention of Mark).

The combination of Mark and Maes et al does not teach user the input means comprising of a signature identification method. However Fung et al. discloses an ID system, which authorizes user with biometric input, including signature or other writing (col 5 section 0060). The secure access card uses the signature information of the user as authentication information to authorize the user to use the requested services. Fung et al teaches the use of biometric data,

including written signature, to authenticate the user who is accessing downloaded content. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Fung et al within the combination of Mark and Maes et al because it would have added another set of data to authenticate the user.

As per claim 20, Mark discloses a tone sequence (DTMF signal, col 5 ln 25-57), comprising of a representation of the captured at least one of a key input, a voice audio input, and a fingerprint input from a user of the secure access card to identify the user thereof (PIN corresponding to input, col 57 ln 13-22, and voice transmitted via encoded DTMF, col 50 ln 55-63).

Mark does not teach user the input means comprising of a signature identification method. However Fung et al. discloses an ID system, which authorizes user with biometric input, including signature or other writing (col 5 section 0060). The secure access card uses the signature information of the user as authentication information to authorize the user to use the requested services. Fung et al teaches the use of biometric data, including written signature, to authenticate the user who is accessing downloaded content. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Fung et al within the system of Mark because it would have added another set of data to authenticate the user.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Allen S. Wu whose telephone number is 703-305-0708. The examiner can normally be reached on Monday-Friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-0900.

Allen S. Wu
Examiner
Art Unit 2131

ASW

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100